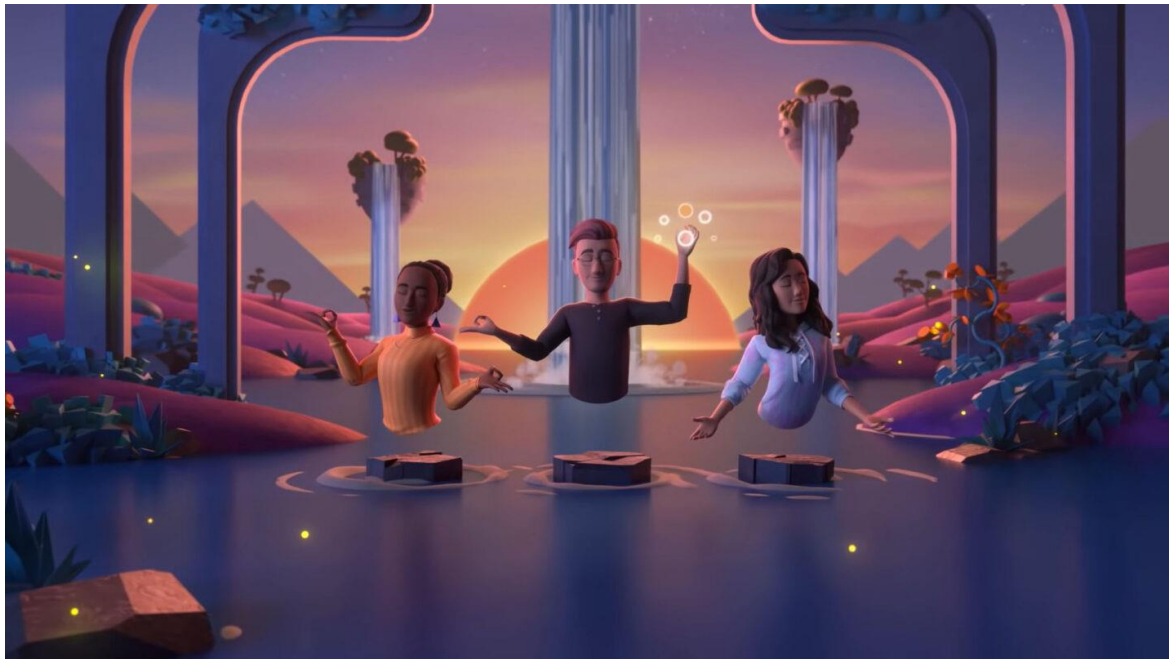
Metaverse/Web3: Technik

Prof. Dr. Stefan Schmid (TU Berlin)



Credits: Yvonne-Anne Pignolet (Dfinity)

Roadmap

- ⇢ Web3 und Metaverse: Vision
- ⇢ Technologie
- ⇢ Herausforderungen

Web3 vs Metaverse

Mögliches Anwendungsszenario

⇢ Web3: Plattform (z.B. Dfinity’s Internet Computer)

⇢ Metaverse: Anwendung auf Web3 (z.B. **Smart Contracts**)

DFINITY

Vision Web3

Web1:
“Lesen”

Web2:
“Posten”
bei Giants

Web3:
“Dezentral Sharen”
(Inhalte und Rechte)

⇢ Web2: Inhalte von Facebook, Whatsapp, … geteilt

⇢ Web3: Jeder kann eigene Inhalte/Code/Rechte (“**Tokens**”) flexibel teilen (“alles sharen”); behalte Kontrolle über Daten selber!

Blockchain

⇢ Es geht um v.a. um **Ownership** und **Governance**: Rechte verteilen und zusammen weiterentwickeln und entscheiden wie es weitergeht

Consensus / BFT

Beispiel

⇢ Facebook heute: ganz kleiner Bruchteil von Facebook Usern haben Shares und können mitbestimmen

⇢ In der Zukunft: “**Involvement**” von (fast) allen Usern? Für Ownership und Governance.

Vision Metaverse

⇢ Computer erzeugte und vernetzte „virtuelle Welt“

⇢ Genauer: Extended reality (XR)
  ⇢ Also Virtual und/oder Augmented Reality (oder hybrid)

⇢ Zugang mit Headset…

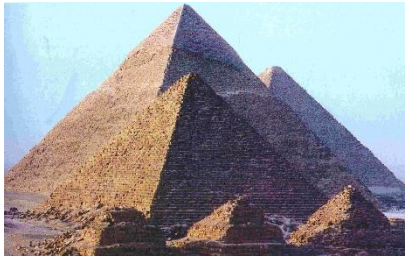
⇢ … aber immer mehr auch mit **haptischen** Technologien (Berührung, Vibrationen, Bewegungen)
  ⇢ Z.B. Gerät das „zieht“

⇢ Mehr als Facebook Meta… und v.a. auch dezentral (Web3)

Herausforderungen

- ⇢ Sicherheit
- ⇢ Performanz
- ⇢ Zentral bei beiden Aspekten: Daten und AI

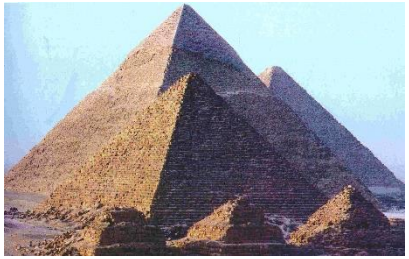
Internet Sicherheit



Internet auf ersten Blick:

- ⇢ Monumental
- ⇢ “Test of Time” bestanden
- ⇢ Soll und kann man nicht ändern

Internet Sicherheit



Internet auf ersten Blick:

- ⇢ Monumental
- ⇢ “Test of Time” bestanden
- ⇢ Soll und kann man nicht ändern

Auf zweiten:

- ⇢ Antik
- ⇢ Anfällig
- ⇢ Immer mehr Attacken

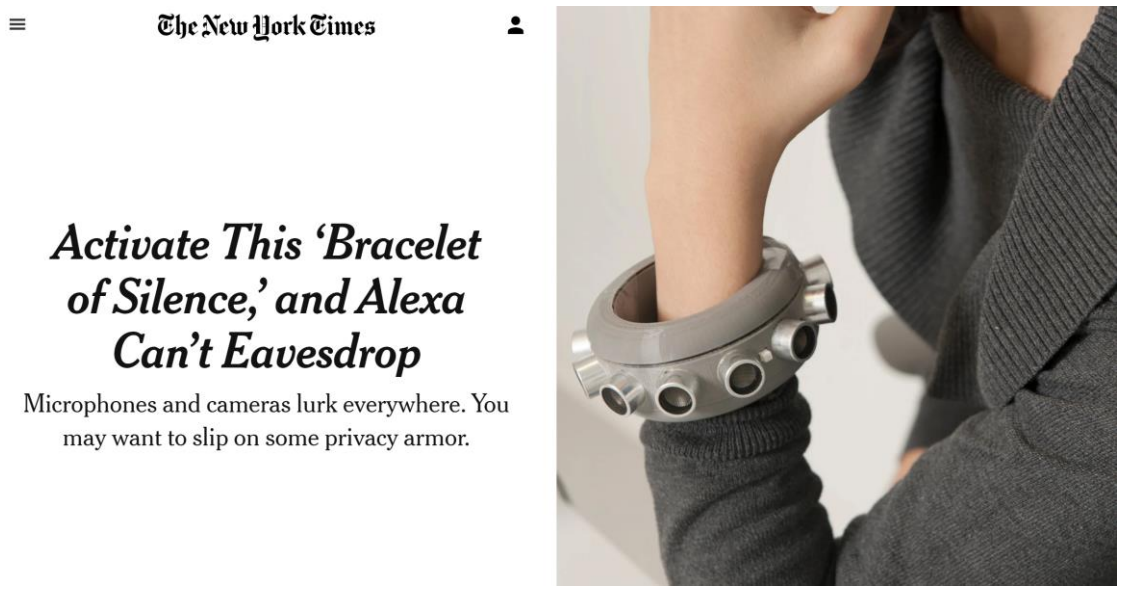
Annahmen

Sicherheitsannahmen haben sich geändert:

⇢ In 80ern: basierend auf **Vertrauen**
⇢ Danny Hillis, TED talk, Feb. 2013, “There were two Dannys. I knew both. Not everyone knew everyone, but there was an atmosphere of trust

Daten schützen heute

Oft kreativ…



February 2020: Wearable microphone jamming.
(https://www.mirror.co.uk/tech/alexa-owners-can-stop-eavesdropping-21539032)

Daten schützen heute

Oft kreativ…

Brille von Scott Urban: reflektiert Infrarot Licht
„blurred“ Gesicht vor Security Kameras

Computation mit Sensitiven Daten

Homomorphic Encryption

⇢ Cloud Berechnungen müssen nicht unsicher sein!

⇢ Beispiel 1: **Homomorphe** Verschlüsselung
Berechnungen auf verschlüsselten Daten!

Computation mit Sensitiven Daten

Homomorphic Encryption

⇢ Cloud Berechnungen müssen nicht unsicher sein!

⇢ Beispiel 1: **Homomorphe** Verschlüsselung
Berechnungen auf verschlüsselten Daten!

f(3),f(5)

f(8)

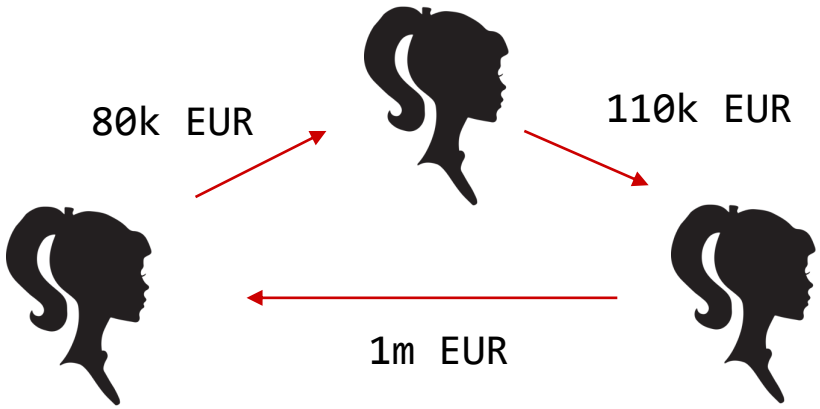
+

Computation mit Sensitiven Daten

Secure Multi-Party Computation

⇢ Verteilte Berechnungen müssen nicht unsicher sein!

⇢ Beispiel: sichere **Multi-Party Computation**
Z.B. verteilt Durchschnittslohn berechnen

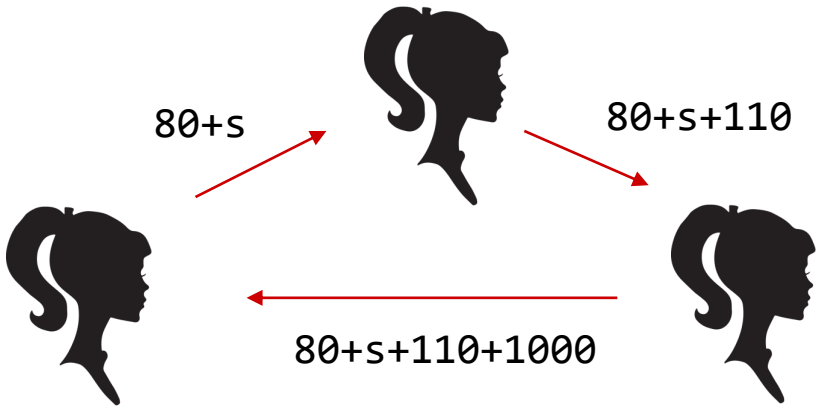


Computation mit Sensitiven Daten

Secure Multi-Party Computation

⇢ Verteilte Berechnungen müssen nicht unsicher sein!

⇢ Beispiel: sichere **Multi-Party Computation**
Z.B. verteilt Durchschnittslohn berechnen



Für (grosses) geheimes s.

Sicheres Cloud Computing

Trusted Executions

⇢ Cloud Berechnungen müssen nicht unsicher sein!

⇢ Beispiel 2: **trusted executions (enclaves)**
sichere Hardware (inkl. Schlüssel), z.B. Intel SGX,
Nano Ledger (für Verwaltung von Crypto oder NFTs)

⇢ Z.B. Challenge-Response Authentifizierung
mit **asymmetrischer Crypto**

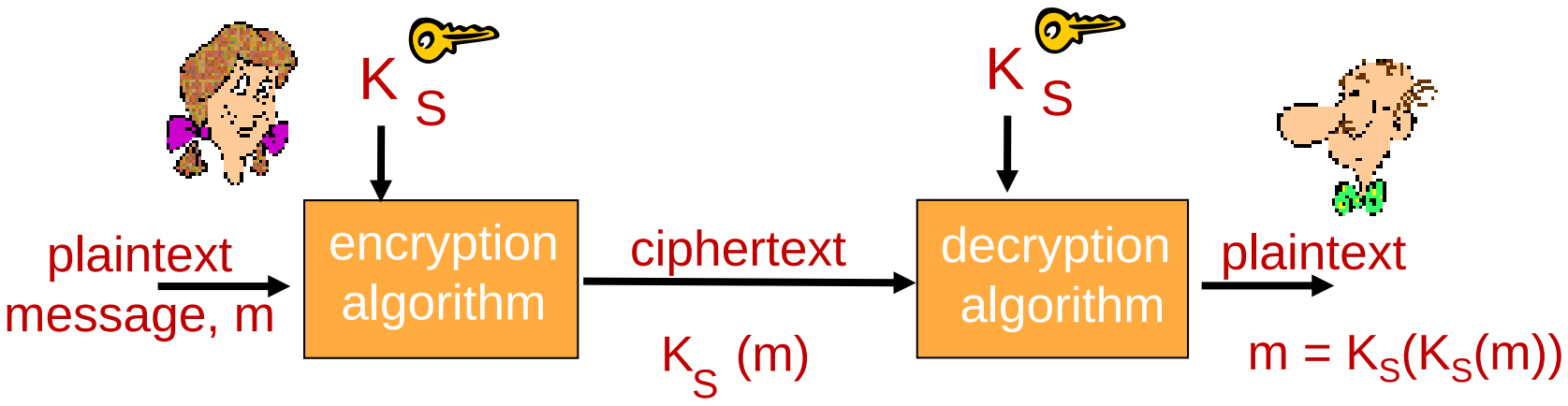
Sicherheitsanforderungen

- Sichere Identitäten (“**identity**”)
  - Anonym oder nicht anonym
  - Vererbbar oder nicht (ownership)
  - Z.B. über **derived keys**

- Digitale Signaturen, nicht abstreitbar (non-repudiation)

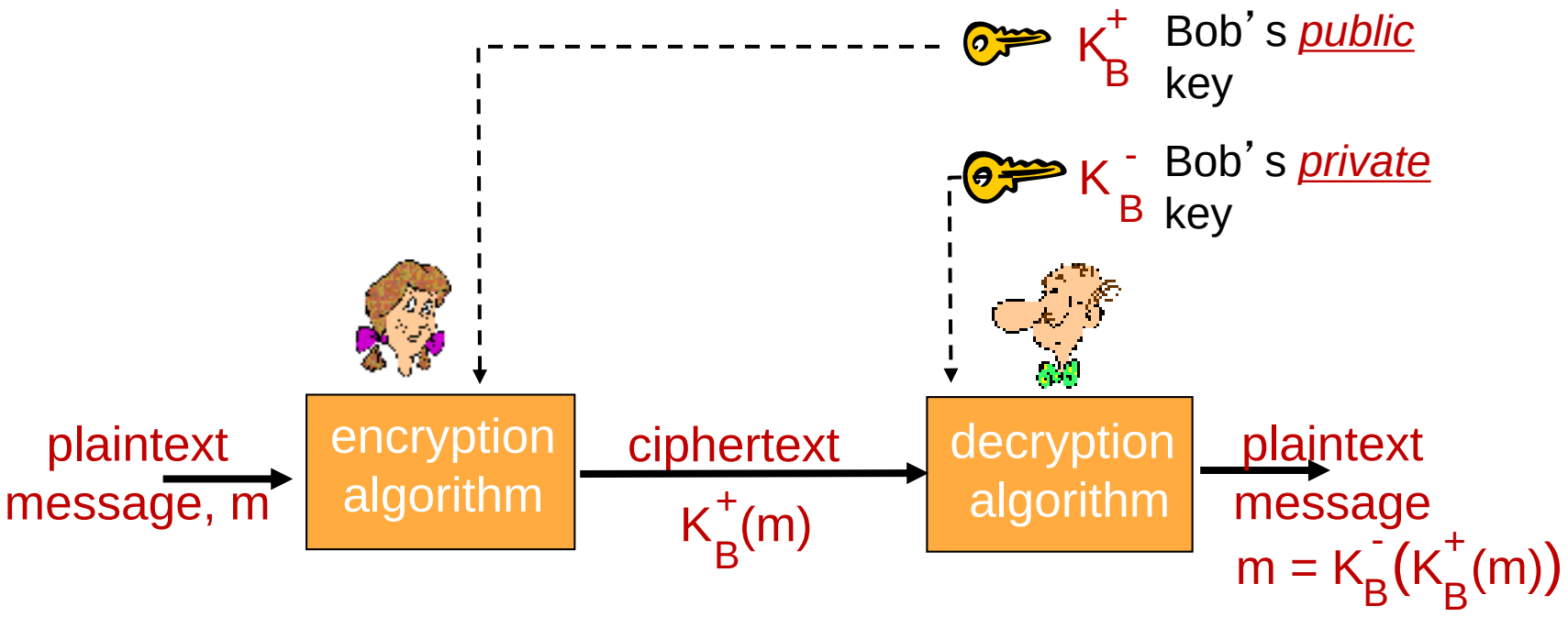
- Mit **asymmetrischer Crypto**

Symmetrische Crypto



- Alice und Bob benutzen gleichen Schlüssel: K_S
  - Zum Verschlüssel und Entschlüsseln (resp. Signieren)
- Problem:
  - Wie sich auf Schlüssel einigen, wie verschicken?
  - Beim Signieren: Drittpersonen können nicht unterscheiden ob Alice oder Bob signiert hat
  - Also **abstreitbar**

Asymmetrische Crypto



- Unterschiedliche Schlüssel und Private Keys
- Wenn Bob mit Private Key signiert, können alle mit seinem Public Key verifizieren, dass er (und nur er) unterschrieben hat

Consensus und Performanz

- ⇢ Wie alle involvieren? Governance mit Consensus/BFT?
- ⇢ Aktuell oft noch ein Flaschenhals, z.B. Consensus nötig um auf Blockchain zu schreiben
- ⇢ Neue Technologien verbessern aber Performanz stark
- ⇢ Z.B. **Offchain Networks** basierend auf Peer-to-Peer Technologien
- ⇢ Herausforderung aber auch: wie sicherstellen dass nicht jemand mehr **Abstimmungsmacht** hat als ihm/ihr zusteht?

Künstliche Intelligenz

- Wichtig an “allen Fronten”
  - Für Performance, NFT designs (status Symbol!)
    bessere Visualisierung, “Bots” im Metaverse …

- Auch ein Ziel von Web3: **Semantic Web**
  - Daten auf dem Internet sollen “machine-readable” werden
  - Erlaubt es Recherchen zu automatisieren

- Gefahren?
  - Viel Forschung zu **Ethical Algorithms**, Explainable AI, …

Conclusio

- ⇢ Vision von dezentralerem Web und Metaverse
- ⇢ Technologien: Sicherheit, Experience (z.B. haptisch), Performanz (z.B. Peer-to-Peer)
- ⇢ Viele (unsichere!) Business Opportunities…
- ⇢ … und viele rechtliche Fragen: Prof. Dr. Paal